Montana State Legislature

Information Security Program
Charter Document

Program Name: Montana Legislative Branch Information Security Program

Department: Office of Legislative Information Technology, Legislative Services Division, Montana Legislative Branch

Focus Area: Information Privacy and Data Protection

Prepared By

Document Owner(s)	Program /Organization Role
Dale Gow	Montana Legislative Branch Information Security Officer

Program Charter Version Control

Version	Date	Action Author	Action Description
1.0	3/20/2008	Dale Gow	Document created
2.0	3/21/2008	Hank Trenk	OLIT Director's review and edit
3.0	3/24/2008	Connie Dixon	Complete document edit
4.0	3/26/2008	Greg Petesch	Legal review, changed ref: 5-11-112 on page 4 to ref: 5-11-405
5.0	4/3/2008	Susan Fox	LSD Director's review and edit

TABLE OF CONTENTS: PAGE:

1 PROGRAM CHARTER PURPOSE

Information is a critical asset for the Legislative Branch of Montana state government. The Legislative Branch's daily operations and the associated delivery of constituent services rely on the confidentiality, integrity, and availability of information.

The growing dependence on information technology and the increased use of information systems and communications networks heighten the risk of compromising the confidentiality, integrity, or availability of certain Legislative Branch information assets. Consequently, the Legislative Branch must ensure that its information assets are consistently protected in a cost-effective manner that effectively reduces the risk of inappropriate exposure, misuse, or loss of data.

The **Office of Legislative Information Technology** (OLIT) provides essential support of information systems and communication networks used by the Legislative Branch, including its online bill status system. Accordingly, OLIT is responsible for the Legislative Branch's Information Security Program.

This Information Security Program Charter serves as the capstone and empowerment document of the Information Security Program for the Legislative Branch. Furthermore, this charter is provided to summarize the Legislative Branch's attitude and philosophy regarding security and to state the specifics of the Information Security Program mission within the Legislative Branch. Additionally, this charter addresses key program management issues, including scope of applicability, executive ownership, management responsibility, accountability, enforcement, and communication processes.

2 PROGRAM EXECUTIVE SUMMARY

The Information Technology Services Division (ITSD) of the Department of Administration provides functional data network connectivity to all branches, departments, and divisions within Montana's state government. Consequently, ITSD is responsible for network security of the State's primary data network, or backbone, and has consequently developed and implemented a variety of security-related mandates[1]. However, in accordance with the Montana Constitution[2], the Legislative Branch is responsible and required to maintain a clear separation of function. Accordingly, OLIT is responsible, among other duties, for ensuring the confidentiality, integrity, and availability of information within the Legislative Branch. As a result, OLIT has appointed the Legislative Branch Information Security Officer (LB ISO) to lead and manage this critical undertaking.

The Legislative Branch's Information Security Program will put into practice a risk management approach for information security. A risk management approach for information security requires

[1] **Data Security and Quality**
The State of Montana is committed to data security and the data quality of personally identifiable information that is either available from or collected by governmental web sites, and has taken reasonable precautions to protect personally identifiable information from loss, misuse or alteration. http://itsd.mt.gov/policy/policies/ENTINT030.asp

[2] **The Constitution of the State of Montana Article III, Section 1. Separation of powers.** The power of the government of this state is divided into three distinct branches--legislative, executive, and judicial. No person or persons charged with the exercise of power properly belonging to one branch shall exercise any power properly belonging to either of the others, except as in this constitution expressly directed or permitted.

the identification, assessment, and mitigation of threats and vulnerabilities to the Legislative Branch's information assets. Consequently, the LB ISO will work in conjunction with the security group of the ITSD in ensuring the greatest possible confidentiality, integrity, and availability of data within the Legislative Branch.

An essential element the Information Security Program is the establishment of appropriate communication, authorization, and management paths for information security issues within Montana's Legislative Branch. Thus, in accordance with section 5-11-405, MCA, this Information Security Program Charter looks to the Legislative Council as the appropriate and authorized body to ratify and adopt the Information Security Policy within the Legislative Branch Computer System Plan. The Legislative Branch Computer System Plan is developed and maintained by the Legislative Branch Computer System Planning Council (CSPC). The CSPC is composed of representatives of the House and Senate and the directors of the legislative agencies who can represent the user needs of each entity. Section 5-11-406, MCA, requires computer hardware and software systems installed by the Senate, the House, and legislative branch agencies must conform to standards established in the legislative branch computer system plan, which makes it the logical document to incorporate the Information Security Program, including the charter and subsequent standards, policies, and procedures.

3 PROGRAM OVERVIEW

In designing the critical elements of the Legislative Branch Information Security Program, the LB ISO has adopted a two-step approach that, while complementary to the security strategy expressed by the ITSD, is fully focused on the unique business practices, requirements, and concerns of the Legislative Branch.

The initial step for the Legislative Branch Information Security Program is to put into practice a Security Program Development Life Cycle[3] methodology intended to create a viable program framework. Thus, the LB ISO has created the Information Security Program development project to initiate this effort. The Information Security Program development project consists of five phases. The phases identified below are foundationally based, but may overlap in the development process.

Phase I: Program Charter and Policy Development

Phase II: Employee Awareness and Education

Phase III: Security Architecture Enhancements

Phase IV: Security Management and Control

Phase V: Security Measurements and Metrics

As the program matures, ultimately at the conclusion of Phase V, the Information Security Program will move into a maintenance stage that subsists on conclusions derived from security incident analysis or security compliance assessments, and there may be a need for refinement of policy and/or procedure, as the situation dictates.

[3] Access - Analyze - Plan - Implement - Assess - Refine

The Legislative Branch Information Security Program intends to incorporate a common hierarchical Security Policy management methodology[4]. This approach documents the intended security strategy ranging from a very high-level statement of purpose (Program Charter) and cascading down to specific procedures or "how-to" documents for individual Legislative Branch information technology administrators and users.

The Legislative Branch Information Security Program intends to pursue a risk management strategy for protecting information transiting through or stored within the Legislative Branch. Information at risk becomes identifiable through the implementation of a suitable set of organizational structures, controls, policies, processes, and procedures. Accordingly, this strategy requires *defining or identifying the controls* for certain activities associated with information management. Ultimately, the goal is for each identified risk to result in a strategy being devised that will provide a *balance between cost to mitigate vulnerabilities and acceptable risk* to Legislative Branch information.

Information exists in a variety of forms. Information may be printed from computer memory, written on paper, stored electronically, transmitted through the postal system or by electronic means, or spoken in conversation. Therefore, establishing the distinction between sensitive and nonsensitive information, as well as where and how that information should be stored, transmitted, or shared, is crucial. For that reason, the selected information security controls associated with how people process and store Legislative Branch information must be all encompassing.

The *ISO/IEC 17799 Code of Practice for Information Security Management* is an accepted international standard and has been adopted by the LB ISO. The following 10 control areas, based on the ISO 17799 Standard, provide a preview outline of expected Legislative Branch Information Security Policy:

1. Infrastructure Security Management
2. Organizational Asset Management
3. Human Resource Security Management
4. Physical and Environmental Security Management
5. Communications and Operations Management
6. Information Access Control Management
7. Information Systems Security Management
8. Information Security Incident Management
9. Business Continuity Management
10. Compliance Management

Furthermore, the LB ISO has chosen to trust certain recommendations made by the National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, for framing certain procedures and guidelines regarding Information Security issues[5].

[4] Charter - Policy - Procedures - Guidelines

[5] The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) has the broad mission of supporting U.S. industry, government, and academia by promoting U.S. innovation and industrial competitiveness through advancement of information technology measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Under the Federal Information Security Management Act, ITL is directed to develop cyber security standards, guidelines, and associated methods and techniques. ITL responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non national-security-related information.

In summary, the Legislative Information Security Program is based on the ISO 17799 Standard for defining policy, and subordinate procedures and guidelines will be supported by NIST recommendations. This tactic provides a comprehensive approach to framing the risk management strategy necessary to protect information within the Legislative Branch. Additionally, this approach corresponds with current efforts under development by ITSD and is therefore complementary to ITSD's effort.

4 PROGRAM SCOPE

This Information Security Program Charter and associated policies, procedures, and guidelines apply to all employees, contractors, part-time and temporary workers, and those employed by others that may perform work on State of Montana Legislative Branch premises or who have been granted access to State of Montana Legislative Branch information or information systems.

5 REVIEW AND REVISION

The State of Montana's Legislative Branch Information Security Program status and its associated policies shall be reviewed at least annually or upon significant changes to the organizational or technical operating environments, in order to assess their adequacy and appropriateness. The review should be conducted by the Computer System Planning Council and incorporated into the Computer System Plan adopted by the Legislative Council.

6 ENFORCEMENT AND EXCEPTION HANDLING

Failure to comply with State of Montana Legislative Branch Information Security Policies, including subordinate procedures, may result in disciplinary actions up to and including termination of employment or termination of contracts for contractors, consultants, and other entities. Furthermore, legal actions (civil or criminal) may be undertaken as appropriate.

Requests for exceptions to State of Montana Legislative Branch Information Security Policies, or subordinate procedures, should be delivered as a formal ***Request for Exception to the Montana Legislative Information Security Program*** and submitted to the LB ISO. The LB ISO will deliver all ***Request for Exception*** to the Computer System Planning Council and any disputes forwarded to the Legislative Council for final determination.

7 APPROVALS

Prepared by: _____

Fredrick “Dale” Gow,
Legislative Branch Information Security Officer

Approved by:

The Information Security Program Charter was approved by motion during the _____ Computer Systems Planning Council.

Adopted by:

The Information Security Program Charter was adopted by motion during the _____ Legislative Council.